3169.66103 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RS

#2

3-11-02

In Re U.S. Patent Application)
)
Applicant: Nobuyuki Koike)
)
Serial No.)
)
Filed: January 14, 2002)
)
For: KEY INFORMATION ISSUING DEVICE, WIRELESS OPERATION DEVICE, AND PROGRAM)
)
Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on January 14, 2002.
Express Label No.: EL 846223023US
Signature: Dale Conner
EXPRESS.WCM
Appr. February 20, 1998

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

Applicant claims foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2001-236869, filed August 3, 2001.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By
Patrick G. Burns
Registration No. 29,367

January 14, 2002
300 South Wacker Drive
Suite 2500
Chicago, IL 60606
(312) 360-0080
Customer Number: **24978**
F:\DATA\WP60\3169\66103\PRIORITY

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ８月 ３日

出願番号
Application Number: 特願２００１－２３６８６９

出願人
Applicant(s): 富士通株式会社

２００１年１０月２６日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願
【整理番号】　0150324
【提出日】　平成13年 8月 3日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
H04N 5/00
H04Q 1/00
【発明の名称】　鍵情報発行装置、無線操作装置、およびプログラム
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　小池　信之
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100089244
【弁理士】
【氏名又は名称】　遠山　勉
【選任した代理人】
【識別番号】　100090516
【弁理士】
【氏名又は名称】　松倉　秀実
【連絡先】　０３－３６６９－６５７１
【手数料の表示】
【予納台帳番号】　012092
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　鍵情報発行装置、無線操作装置、およびプログラム

【特許請求の範囲】

【請求項１】　鍵情報保持装置に鍵情報を発行する鍵情報発行装置であり、

前記鍵情報の発行者を認証する認証部と、

前記鍵情報保持装置に鍵情報を出力する出力部と、

発行された鍵情報を前記鍵情報保持装置に対応付けて記録する記録部とを備え、認証された発行者の指示により鍵情報を発行する鍵情報発行装置。

【請求項２】　前記鍵情報保持装置は、情報機器に無線で接続される無線操作装置であり、前記鍵情報発行装置に接触して鍵情報を入力する鍵情報入力部を有しており、

前記出力部は、前記鍵情報入力部と接触して鍵情報を出力する接触部を有し、その接触部を介して鍵情報を発行する請求項１記載の鍵情報発行装置。

【請求項３】　情報機器に無線で接続される無線操作装置であり、

情報を暗号化するための鍵情報を入力する鍵情報入力部と、

前記鍵情報を記録する記録部と、

利用者の操作を検出する操作部と、

前記操作による入力情報を前記鍵情報により暗号化する暗号化部と、

暗号化された入力情報を情報機器に送信する送信部とを備える無線操作装置。

【請求項４】　前記鍵情報保持装置は、所定領域の施錠を開放する電子鍵である請求項１記載の鍵情報発行装置。

【請求項５】　コンピュータに、鍵情報保持装置に発行される鍵情報を管理させるプログラムであり、

前記鍵情報の発行者を認証するステップと、

鍵情報を生成するステップと、

前記鍵情報保持装置に鍵情報を出力するステップと、

発行された鍵情報を前記鍵情報保持装置に対応付けて記録するステップとを有するプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、鍵情報の処理技術に関するものである。

【０００２】

【従来の技術】

従来から、人間社会の様々な場面で鍵情報が使用されている。例えば、情報の秘匿を行う必要があるデータ通信においては、暗号鍵が使用される。また、建物やオフィスの鍵として、鍵穴の形状に合わせた金属鍵に代えて磁気ストライプに鍵の情報を記録したものが使用されている。以下、暗号鍵や建物等の鍵の情報を合わせて鍵情報という。

【０００３】

【発明が解決しようとする課題】

しかし、従来のシステムでは、このような鍵情報を簡易に変更し、再発行することはできなかった。あるいは、再発行可能であっても暗号を記憶しておく必要があるため、再発行を行うことは再度の記憶を必要とし、煩雑であった。このため、パーソナルコンピュータ等の情報機器間の通信において暗号鍵が使用されることはあっても、日常生活で使用する簡易な通信、例えば、テレビ受像機とその無線のリモートコントローラ（以下単に無線リモコンという）の間の通信、無線キーボードとパーソナルコンピュータの間の通信において暗号鍵が用いられることはなかった。

【０００４】

しかし、今後、例えば、無線リモコンや無線キーボードを介したホームバンキングなどをする場合と考えると、これらの通信を暗号化することは望ましい。銀行口座のパスワード等が傍受される場合もあるからである。

【０００５】

そのような暗号を通信相手に解読させるためには、通信する機器間で暗号の申し合わせが必要である。したがって、テレビ受像機と無線リモコンとの間、パーソナルコンピュータと無線キーボードとの間で簡易、安全に暗号鍵を発行できるシステムが必要になる。

【０００６】

他方、例えば、建物やオフィス等において錠の開閉に使用される磁気ストライプ形式やＩＣカードによる鍵（以下、これらを電子キーという）は、持ち運びに便利な分だけ、紛失・盗難の対象になりやすい。このような鍵は、例えば、鍵（または建物）の管理会社のセンタで一括されている。

【０００７】

このため、このような鍵を紛失すると、その建物やオフィスを使用するために配布されたすべての鍵を回収し、鍵情報を書き直さなければならない。このような鍵の回収と再発行の手間は非常に煩わしいものであった。

【０００８】

本発明はこのような従来の技術の問題点に鑑みてなされたものである。すなわち、本発明の課題は、情報機器と無線操作装置との間の通信において傍受からの十分な安全性を確保することにある。

【０００９】

また、本発明の課題は、鍵情報を保持する鍵情報保持装置に対して簡易に鍵情報を発行することにある。

【００１０】

また、本発明の課題は、そのような鍵情報の発行において、傍受からの十分な安全性を確保することにある。

【００１１】

【課題を解決するための手段】

本発明は前記課題を解決するために、以下の手段を採用した。すなわち、本発明は、鍵情報保持装置（２、２Ａ、２Ｂ）に鍵情報を発行する鍵情報発行装置（１、１Ａ、１Ｂ）であり、

鍵情報の発行者を認証する認証部（１４、３）と、

上記鍵情報保持装置に鍵情報を出力する出力部（１３）と、

発行された鍵情報を上記鍵情報保持装置に対応付けて記録する記録部（１１）とを備え、認証された発行者の指示により鍵情報を発行するものである。

【００１２】

好ましくは、上記鍵情報保持装置（２、２Ａ、２Ｂ）は、情報機器に無線で接続される無線操作装置（２、２Ａ）であり、接触して情報を入力する鍵情報入力部（２３）を有しており、

上記出力部（１３）は、その鍵情報入力部（２３）と接触して鍵情報を出力する接触部を有し、その接触部を介して鍵情報を発行するものでもよい。

【００１３】

好ましくは、上記鍵情報保持装置（２、２Ａ、２Ｂ）は、情報機器に無線で接続される無線操作装置（２、２Ａ）であり、記録媒体から情報を入力する媒体入力部を有しており、

上記出力部（１３）は、その記録媒体に情報書き込む記録媒体書き込み部を有し、その記録媒体を介して鍵情報を発行してもよい。

【００１４】

好ましくは、上記鍵情報保持装置（２、２Ａ、２Ｂ）は、情報機器に無線で接続される無線操作装置（２、２Ａ）であり、所定距離外では通信できない近接通信部を有しており、

上記出力部（１３）は、上記鍵情報保持装置と所定距離外では通信できない近接通信部を有し、その近接通信部を介して鍵情報を発行するものでもよい。

【００１５】

好ましくは、上記鍵情報発行装置（１、１Ａ）は、上記鍵情報保持装置からの無線信号を受信する受信部（１３）と、

その無線信号に含まれる、上記暗号鍵情報により暗号化された情報を復号する復号部（１１）とをさらに備えてもよい。

【００１６】

また、本発明は、情報機器に無線で接続される無線操作装置（２、２Ａ）であり、

情報を暗号化するための鍵情報を入力する鍵情報入力部（２３）と、

その鍵情報を記録する記録部（２４）と、

利用者の操作を検出する操作部（２２）と、

その操作による入力情報を上記鍵情報により暗号化する暗号化部（２１）と、

暗号化された入力情報を情報機器に送信する送信部（２５）とを備えるものでもよい。

【００１７】

好ましくは、上記鍵情報入力部（２３）は、鍵情報を接触して入力する接触部を有してもよい。

【００１８】

好ましくは、上記鍵情報入力部（２３）は、記録媒体から情報を入力する媒体入力部を有してもよい。

【００１９】

好ましくは、上記鍵情報入力部（２３）は、所定距離外では通信できない近接通信部を有してもよい。

【００２０】

好ましくは、上記無線操作装置（２、２Ａ）は、暗号化の有無を設定する設定部（２７）をさらに備え、

上記暗号化部（２１）は、暗号化が指示されているときに入力情報を暗号化するようにしてもよい。

【００２１】

また、本発明は、情報機器に無線で接続される無線操作装置（２、２Ａ）であり、

利用者の操作を検出する操作部（２２）と、

上記操作による入力情報を送信する送信部（２５）と、

送信した入力情報に対する上記情報機器からの応答信号の有無を確認する確認部（２１）とを備え、上記応答信号が得られない場合に、入力情報の送信を停止してもよい。

【００２２】

また、本発明は、情報機器に無線で接続される無線操作装置（２、２Ａ）であり、

利用者の操作を検出し、入力情報を生成する操作部（２２）と、

上記入力情報を模擬した模擬情報を発生する模擬情報発生部（２１）と、

上記入力情報または模擬情報を送信する送信部（２５）とを備えるものでもよい。

【００２３】

好ましくは、上記模擬情報は、利用者による操作の有無に拘わらず送信されるようにしてもよい（Ｓ２Ａ－Ｓ２Ｃ）。

【００２４】

好ましくは、上記鍵情報保持装置（２、２Ａ、２Ｂ）は、所定領域の施錠を開放する電子鍵（２Ｂ）であってもよい。

【００２５】

また、本発明は、鍵情報保持装置に発行される鍵情報を管理する方法であり、

鍵情報の発行者を認証するステップ（Ｓ１０－Ｓ１１）と、

鍵情報を生成するステップ（Ｓ１５）と、

上記鍵情報保持装置に鍵情報を出力するステップ（Ｓ１６）と、

発行された鍵情報を上記鍵情報保持装置に対応付けて記録するステップ（Ｓ１Ｂ）とを有するものでもよい。

【００２６】

また、本発明は、コンピュータに、以上いずれかの機能を実現させるプログラムであってもよい。また、本発明は、そのようなプログラムをコンピュータ読み取り可能な記録媒体に記録したものでもよい。

【００２７】

【発明の実施の形態】

以下、図面を参照して本発明の好適な実施の形態を説明する。

【００２８】

《第１実施形態》

以下、本発明の第１実施形態を図１から図８の図面に基いて説明する。図１は第１実施形態に係る情報システムの全体図であり、図２は、図１に示す無線リモコン２のブロック図であり、図３は、図１に示す本体部１と無線リモコン２との間で交信されるパケットのデータ構造図であり、図４は、本体部１から無線リモコン２へ暗号鍵を配布する手順を示すフローチャートであり、図５は、無線リモコ

ン２の動作時の処理を示すフローチャートであり、図８は、本体部１の受信動作時の処理を示すフローチャートである。

【００２９】

＜機能概要＞

本実施形態の情報システムは、無線通信によるリモコンにより操作される。この情報システムは、ユーザを認証し、ユーザの使用するリモコンごとに暗号鍵を発行する。このとき、情報システムは、リモコンごとに発行した暗号鍵を記録しておく。

【００３０】

ユーザがリモコンにより情報システムを操作する場合、上記暗号鍵により、入力情報が暗号化される。そして、リモコンは、情報システムに交信開始要求を送信し、暗号化された入力情報を送信する。

【００３１】

情報システムは、リモコンから送信される交信開始要求により、リモコンを識別する。そして、情報システムは、記録しておいた暗号鍵のうち、そのリモコンに対して発行したものを参照する。そして、その暗号鍵で入力情報を復号し、ユーザの操作を検出する。

【００３２】

この暗号鍵配布の手順は、以下の通りである。

（１）情報システムの本体側装置は、ユーザ本人の認証を実行する。この処理は、ユーザが鍵情報の配布作業資格を有するか否かの確認作業である。

（２）次に、本体側装置は、リモコンの本体側装置への近接を確認する。

（３）次に本体側装置は、暗号鍵（例えば、乱数）を発生する。

（４）本体側の装置は、傍受を防止した安全な通信路により暗号鍵をリモコンへ送信する。

（５）本体側の装置は、リモコンが安全に暗号鍵を受け取ったことを確認する。

【００３３】

＜全体構成＞

図１に、本情報システムの全体構成図を示す。図１に示すように、この情報シス

テムは、本体側装置（以下本体部１という）と無線リモコン２とから構成される。

【００３４】

本体部１は、不図示のネットワークを通じて外部システムと通信可能な情報処理装置であり、例えば、パーソナルコンピュータ（以下、パソコンと省略する）、デジタルテレビ、セットトップボックス等である。

【００３５】

この本体部１は、パソコン相当機能部分１１、リモコン近接確認部分１２、リモコン通信部分１３、および認証機能部分１４を有している。

【００３６】

パソコン相当機能部分１１は、情報処理機能を提供するＣＰＵ、情報を記憶するメモリ、ネットワークにアクセスする通信インターフェース等を有している。このような構成および作用は、現在では、広く知られているので、その説明を省略する。パソコン相当機能部分１１は、このような構成により、本体部１を制御し、各種の情報処理機能を提供する。

【００３７】

例えば、パソコン相当機能部分１１は、無線リモコンに送信する暗号鍵を生成する。この暗号鍵生成では、所定の方式で乱数（あるいは素数）を生成する。生成した暗号鍵は遠隔通信時に必要なので本体部１の不図示のメモリに記録・保存される。

【００３８】

パソコン相当機能部分１１は、この鍵に、無線リモコン２を識別するためのIDを含める。そして、パソコン相当機能部分１１は、そのような無線リモコン２のIDと配布した暗号鍵との対応表を記録しておく。

【００３９】

このIDとしては無線リモコン２の製造番号を用いてもよい。また、乱数を用いて無線リモコンのIDを発生させても良い。これによって、本情報システムは、複数のリモコンを管理できる。ただし、リモコンを複数使わない場合はこのIDは不要である。その他にも必要な情報があれば、暗号鍵の一部に含めればよい。

【００４０】

また、パソコン相当機能部分１１は、無線リモコン２が確実に暗号鍵を受け取ったかどうかを確認する。その場合、例えば、無線リモコン２から単純に暗号鍵そのものを返信させ、パソコン相当機能部分１１が確認すればよい。また、無線リモコン２からチェックサムの返信だけを行うようにしてもよい。暗号鍵の送信が失敗していたとしても、無線リモコン２が使えなくなるだけであり、配布手順をやり直すことで使えるようになる。したがって、暗号鍵送信処理の信頼性が十分高ければ、無線リモコン２が確実に暗号鍵を受け取ったかどうかの確認を省略してもよい。

【００４１】

認証機能部分１４は、ユーザ本人を認証する機能を提供する。認証方式としては、指紋・声紋等の生体認証、暗証番号による認証、パスワード認証など、要求される機密度と実現コストに応じた方式を選択できる。

【００４２】

認証機能部分１４は、このような認証方式により、暗号鍵の無線リモコン２への配布を指示する資格がユーザにあるかどうかを確認する。ユーザに暗号鍵の配布を指示する資格がなければ、それが判明した時点で本体部１は処理を中断する。

【００４３】

リモコン近接確認部分１２は、例えば、押しボタン等である。ユーザは、無線リモコン２を本体部１に近接させたとき、このリモコン近接確認部分１２を操作する（例えば、押しボタンを押下する）。これにより、本体部１は、無線リモコン２の近接を認識する。

【００４４】

この状態で、本体部１は、無線リモコン２と有線通信または微弱電波による無線通信で通信する。図１の下部に、そのような状態の本体部１と無線リモコン２を例示する。

【００４５】

リモコン通信部分１３は、無線リモコン２に暗号鍵を送信する機能を提供する

。このリモコン通信部分１３は、通信インターフェースと通信プログラムにより構成される。通信インターフェースとして、RS232Cなどのシリアル方式、セントロニクス規格準拠のパラレル方式、その他の有線方式のインターフェースを使用できる。

【００４６】

このように、本情報システムでは、暗号鍵送信用として、無線通信インターフェースと別個に、傍受されにくいように有線方式を用いる。なお、無線通信インターフェースは、例えば、赤外線受光部、無線ＬＡＮインターフェース等である。ただし、電磁シールドなどを併用することにより、暗号鍵の送信に、無線通信を用いてもよい。

【００４７】

また、所定距離以上離れて通信できない近距離無線方式などを使用してもよい。その場合、リモコン通信部分１３は、暗号鍵を送信する機能と、無線リモコン２からの暗号化された操作信号を受信する機能の双方を兼用すればよい。

【００４８】

この場合、上記シールドとともに、近接時には送信出力を絞る等の傍受対策をすればよい。なお、以上のような鍵情報配信におけるデータフォーマットに限定はない。

【００４９】

図２に、無線リモコン２のブロック図を示す。図２のように無線リモコン２は、無線リモコン２の各部を制御する処理装置２１と、ユーザによる情報システムへの操作を検出し、入力情報を生成するキーボード２２と、情報システムの本体部１から暗号鍵を受信する暗号鍵受信部２３と、処理装置２１により情報を書き込まれ、または読み出されるメモリ２４と、処理装置２１の指示により無線通信で情報を送受信する送受信装置２５と、処理装置２１の指示により各種情報を表示する表示装置２６と、暗号化の実行の有無を指定する暗号化オン／オフスイッチ２７と、無線リモコン２に電力を供給する電源部（電池）とを有している。

【００５０】

処理装置２１は、例えば、マイクロプロセッサである。処理装置２１は、メモ

リ２４にロードされた制御プログラムを実行し、無線リモコン２の機能を提供する。例えば、処理装置２１は、暗号鍵受信部２３を通じて本体部１から暗号鍵を受信する。また、処理装置２１は、受信した暗号鍵を用いて、本体部１に送信する情報を暗号化する。

【００５１】

キーボード２２は、英数字等のキーの他、各種ボタン類、オン／オフスイッチ等を含む。ユーザは、これらのキー、ボタン、スイッチを操作し、情報システムに対する指示を入力する。

【００５２】

暗号鍵受信部２３は、上述の本体部１のリモコン通信部分１３に対応する通信インターフェースである。

【００５３】

メモリ２４は、ランダムアクセスメモリ（ＲＡＭ）およびリードオンリーメモリ（ＲＯＭ）から構成される。メモリ２４には、処理措置２１で実行されるプログラムや、処理装置２１が使用するテーブル等が格納される。

【００５４】

送受信装置２５は、本体部１と無線通信を行う通信インターフェースである。これは、例えば、赤外線発光部と赤外線受光部、無線ＬＡＮインターフェース等である。

【００５５】

表示装置２６は、無線リモコン２６の動作状態等を表示する。例えば、表示装置２６は、電源ランプ等である。

【００５６】

暗号化オン／オフスイッチ（図２には、暗号化On／Offスイッチと記載）２７は、処理装置２１において情報を暗号化するか否かを指定する。これは、例えば、テレビ受像機等との通信においては、情報を暗号化する必要があるが、エアコンの操作信号を暗号化する必要がない（エアコンの制御部が暗号化に対応していない）等の場合でも、本無線リモコン２を汎用的に使用するために設けられている。ユーザは、無線リモコン２で操作する対象に応じて暗号化のオン／オフを暗

号化オン／オフスイッチ２７により設定する。

【００５７】

＜データ構造＞

図３に、本体部１と、無線リモコン２との間で授受される無線通信データ（以下、このような無線通信データをパケットと呼ぶ）のデータ構造例を示す。図３に示すように、このようなパケットととして、本情報システムでは、交信開始パケット、交信許可パケット、ボタン情報・ダミーパケット、および受信確認パケットが用意されている。

【００５８】

交信開始パケットは、無線リモコン２から本体部１へ交信開始を要求するパケットである。図３に示すように、交信開始パケットは、ヘッダ、パケットＩＤ、リモコンＩＤ、ダミーデータおよびチェックサムの各格納部を有している。

【００５９】

ヘッダは、本情報システムにおいて本体部１と無線リモコン２との間で交信されるパケットであることを示すビット列である。図３では、ヘッダとして”５５ＡＡ”というビット列（１６進数）が例示されている。

【００６０】

パケットＩＤは、パケットの種類を示す番号である。図３では、交信開始パケットには、０００１というＩＤが指定されている。

【００６１】

交信開始パケットのダミーデータは、交信開始パケットの未使用領域を埋めるビット列である。また、チェックサムは、パケット受信時のデータの正当性を確認するための情報である。

【００６２】

交信許可パケットは、無線リモコン２からの交信開始パケットに応答し、本体部１から無線リモコン２へ交信許可を通知するパケットである。図３に示すように、交信許可パケットは、ヘッダ、パケットＩＤ、リモコンＩＤ、セッションＩＤ、ダミーデータおよびチェックサムの各格納部を有している。

【００６３】

これらのうち、ヘッダ、パケットＩＤ、リモコンＩＤ、ダミーデータおよびチェックサムは、交信許可パケットと同様である。また、セッションＩＤは、受信許可また、受信確認のたびに本体部１から無線リモコン２に通知される。無線リモコン２は、受信済みの鍵情報とこのセッションＩＤにより、入力情報を暗号化する。

【００６４】

ボタン情報・ダミーデータパケットは、ボタン情報パケットおよびダミーパケットに分類される。ボタン情報パケットは、無線リモコン２から本体部１へ、ボタン情報（ユーザが操作したボタンの入力情報）を送信するパケットである。また、ダミーパケットは、ダミーデータを送信するパケットである。

【００６５】

図３に示すように、ボタン情報・ダミーパケットは、ヘッダ、パケットＩＤ、リモコンＩＤ、暗号化されたボタン情報またはダミーデータおよびチェックサムの各格納部を有している。

【００６６】

このうち、暗号化されたボタン情報とは、ユーザが無線リモコン２を操作したときの入力情報である。このボタン情報は、予め本体部１から無線リモコン２へ送信された暗号鍵と上記セッションＩＤとにより暗号化されている。また、ダミーパケットは、ボタン情報パケットを第三者が傍受することを防止するためのパケットである。ダミーパケットは、ボタン情報を模擬したダミーデータを有している。ダミーパケットは、ボタン情報パケットの前後に不特定数送信される。

【００６７】

受信確認パケットは、無線リモコン２からのボタン情報・ダミーパケットに応答し、本体部１から無線リモコン２へ受信確認を通知するパケットである。図３に示すように、受信確認パケットは、ヘッダ、パケットＩＤ、リモコンＩＤ、受信パケットのチェックサム、次セッションＩＤ、およびチェックサムの各格納部を有している。

【００６８】

このうち、受信パケットのチェックサムは、前のセッションで受信したパケッ

トのチェックサムである。また、次セッションＩＤは、次にボタン情報を暗号化するときに使用される。

【００６９】

＜作用＞

図４は、暗号鍵配布手順の例を示すフローチャートである。この処理は、暗号鍵を本体部１から無線リモコン２に送信するときに、本体部１（パソコン相当機能部分１１）で実行されるプログラムの処理を示している。

【００７０】

この処理では、本体部１は、まず、ユーザ認証を実行する（Ｓ１０）。ユーザ認証は、リモコンＩＤの読み取り、ユーザからの認証情報の読み取り、およびその認証情報の確認からなる。ユーザからの認証情報は、指紋、声紋、暗唱番号、またはパスワード等である。

【００７１】

次に、その認証結果に基づき、本体部１は、ユーザが暗号鍵の配布を受ける資格があるか、否かを判定する（Ｓ１１）。この判定は、入力された認証情報と、本体部１に登録されている認証情報との比較である。本体部１は、ユーザに資格がないと判定すると、不正ユーザであるとして処理を終了する。

【００７２】

一方、ユーザに資格がある場合、次に、本体部１は、無線リモコン２が近接されるのを待つ（Ｓ１２）。そして、本体部１は、無線リモコン２が近接されたか否かを判定する（Ｓ１３）。

【００７３】

そして、無線リモコン２が近接していない場合、本体部１は、時間切れか否かを判定する（Ｓ１４）。時間切れでない場合、本体部１は、制御をＳ１２に戻す。一方、時間切れの場合、本体部１は、処理を終了する。

【００７４】

Ｓ１３の判定で、リモコンが近接されている場合、本体部１は暗号鍵を生成する（Ｓ１５）。次に、本体部１は、暗号鍵を無線リモコン２に送信する（Ｓ１６）。

【００７５】

次に、本体部１は、リモコンの応答を待つ（Ｓ１７）。応答がない場合、本体部１は、時間切れか否かを判定する（Ｓ１９）。そして、時間切れでない場合、本体部１は、制御をＳ１７に戻す。一方、時間切れの場合、本体部１は、処理を終了する。

【００７６】

Ｓ１８の判定で、応答があった場合、本体部１は正常な応答であるか否かを判定する（Ｓ１Ａ）。正常な応答でない場合、本体部１は、制御をＳ１２に戻し、同様の処理を繰り返す。

【００７７】

Ｓ１Ａの判定で、正常な応答であると判定された場合、本体部１は、リモコンＩＤと暗号鍵の対応表を作成・更新する（Ｓ１Ｂ）。その後、本体部１は、処理を終了する。

【００７８】

図５に、リモコン動作のフローチャートを示す。この処理は、無線リモコン２の処理装置２１で実行されるプログラムの処理を示している。この処理は、無線リモコン２に電源が投入されたとき、または、不図示のリセットボタンが押下されたときに実行される。

【００７９】

この処理では、まず、無線リモコン２は、自身を初期化し、暗号鍵受信待ちの状態になる（Ｓ２０）。次に、無線リモコン２は、暗号鍵の受信が完了したか否かを判定する（Ｓ２１）。

【００８０】

暗号鍵の受信が完了すると、無線リモコン２は、自身のリモコンＩＤとともに、受信した暗号鍵を保存し、受信完了応答を送出する（Ｓ２２）。その後、無線リモコン２は、休止状態になる（Ｓ２３）。この休止状態は、次に、新たな暗号鍵が送信されるか、または、ユーザのボタン操作を検出するまで続く。

【００８１】

すなわち、暗号鍵の受信が開始すると、無線リモコン２は、制御をＳ２１に戻

し、受信完了を確認する。一方、ユーザのボタン操作を検出すると、無線リモコン２は、交信開始パケットを送出する（Ｓ２４）。

【００８２】

そして、無線リモコン２は、交信許可パケットを待つ（Ｓ２５）。そして、所定時間待っても本体部１からの交信許可パケットが受信できない場合、無線リモコン２は、休止状態（Ｓ２３）に移行する。

【００８３】

一方、交信許可パケットを受信した場合、無線リモコン２は、ボタン情報暗号化を実行する（Ｓ２７）。すなわち、無線リモコン２は、ユーザのボタン操作による入力情報を暗号化する。

【００８４】

次に、無線リモコン２は、ダミーパケットを送出する（Ｓ２８）。このダミーパケット送出回数は不定回数（ランダム）である。

【００８５】

次に、無線リモコン２は、ボタン情報パケットを送出する（Ｓ２９）。次に、無線リモコン２は、ダミーパケットを送出する（Ｓ２Ａ）。このダミーパケット送出回数も不定回数（ランダム）である。

【００８６】

次に、無線リモコン２は、さらに、ボタン操作があったか否かを判定する（Ｓ２Ｂ）。さらに、ボタン操作があった場合、無線リモコン２は、Ｓ２７に制御を戻す。

【００８７】

一方、次のボタン操作がなかった場合、無線リモコン２は、時間切れか否かを判定する（Ｓ２Ｃ）。時間切れでない場合、無線リモコン２は、制御をＳ２Ａに戻す。これにより、ユーザが無線リモコン２を操作しなくても、時間切れになるまでの時間、ダミーパケットが不定回数送信される。一方、時間切れの場合、無線リモコン２は、休止状態（Ｓ２３）に移行する。

【００８８】

図６にボタン情報暗号化（図５のＳ２７）の処理の詳細を示す。この処理では

、無線リモコン２は、まず、暗号化オン／オフスイッチ２７がオンか否かを判定する（Ｓ２７０）。

【００８９】

暗号化オン／オフスイッチ２７がオフの場合、無線リモコン２は、ボタン情報暗号化の処理を終了する。一方、暗号化オン／オフスイッチ２７がオンの場合、無線リモコン２は、鍵情報を読み出す（Ｓ２７１）。

【００９０】

次に、無線リモコン２は、セッションＩＤを読み出す（Ｓ２７２）。このセッションＩＤは、交信許可パケットまたは受信確認パケット（図３参照）により入手したものである。

【００９１】

次に、無線リモコン２は、上記鍵情報とセッションＩＤにより、入力情報を暗号化する。その後、無線リモコン２は、ボタン情報暗号化の処理を終了する。

【００９２】

図７に、ボタン情報パケット、ダミーパケット送出処理（図５のＳ２８、Ｓ２９またはＳ２Ａ）の詳細を示す。

【００９３】

この処理では、まず、無線リモコン２は、パケット（ボタン情報パケットまたはダミーパケット）を送出する（Ｓ４１）。

【００９４】

次に、無線リモコン２は、受信確認パケットを待つ（Ｓ４２）。そして、無線リモコン２は、受信確認パケットが受信されたか否かを判定する（Ｓ４３）。受信確認パケットが受信された場合、無線リモコン２は、次の処理へ制御を進める。

【００９５】

一方、Ｓ４３の判定で、受信確認パケットが受信できていないと判定した場合、無線リモコン２は、時間切れか否かを判定する（Ｓ４４）。時間切れでない場合、無線リモコン２は、Ｓ４２へ制御を戻す。一方、Ｓ４４の判定で時間切れであると判定された場合、無線リモコン２は、休止状態へ移行する。

【００９６】

図８に、本体部１の受信動作のフローチャートを示す。この処理が開始すると、本体部１は、交信開始パケット受信待ちの状態になる（Ｓ３０）。そして、本体部１は、交信開始パケットの受信が完了したか否かを判定する（Ｓ３１）。

【００９７】

そして、交信開始パケットの受信が完了すると、無線リモコン２は、受信したリモコンＩＤ（図６には、単にＩＤと記載）と、対応表（図４の１Ｂで作成・交信したもの）とを照らし合わせる（Ｓ３２）。

【００９８】

次に、本体部１は、受信したリモコンＩＤが正規のものか否かを判定する（Ｓ３３）。受信したリモコンＩＤが正規のものでない場合、本体部１は、Ｓ３０に制御を戻す。

【００９９】

一方、受信したリモコンＩＤが正規のものの場合、本体部１は、交信許可パケットを送出する（Ｓ３４）。次に、本体部１は、ボタン情報・ダミーパケットの受信待ちの状態になる。そして、本体部１は、ボタン情報・ダミーパケットの受信が完了したか否かを判定する（Ｓ３６）。

【０１００】

本体部１は、ボタン情報・ダミーパケットの受信が完了すると、受信確認パケットを送出し、さらに、復号処理を実行する（Ｓ３７）。

【０１０１】

次に、本体部１は、受信したパケットがダミーパケットか否かを判定する（Ｓ３８）。受信したパケットがダミーパケットの場合、本体部１は、Ｓ３５に制御を戻す。

【０１０２】

受信したパケットがダミーパケットでない場合、本体部１は、ボタン情報を取りこむ（Ｓ３９）。その後、本体部１は、Ｓ３５に制御を戻す。

【０１０３】

＜実施例の効果＞

以上述べたように、本実施形態の情報システムによれば、無線リモコン２による本体部１への操作、あるいは、情報システムへの操作において、無線リモコン２のボタン情報が暗号化される。このため、無線リモコン２を介した情報システムの操作において、その操作信号を第三者に傍受される可能性を低下させることができる。

【０１０４】

またその際、本情報システムによれば、無線リモコン２が本体部１に接触した有線通信または近接した微弱電波による通信で、本体部１から無線リモコン２に暗号鍵が配信される。このため、暗号鍵そのものを第三者に傍受される危険性を低下させることができる。

【０１０５】

また、本実施形態の情報システムによれば、例えば、交信開始パケットと、これに対する応答パケットのように、所定のシェイクハンド手続により、情報が交信される。このため、無線リモコンによる情報システムの操作において、操作信号を第三者に傍受される危険性を低下させることができる。

【０１０６】

また、本実施形態の情報システムによれば、例えば、ボタン情報パケットの送信の前後にダミーパケットが送信される。このため、無線リモコン２による情報システムの操作において、操作信号を第三者に傍受される危険性を低下させることができる。

【０１０７】

＜変形例＞

上記実施形態では、図３に示したようなパケットにより本体部１と無線リモコン２とが交信した。しかし、本発明の実施は、そのような構成や手順には限定されない。例えば、交信開始パケットでは、基本的には、リモコンＩＤが伝達できればよく、ヘッダ、パケットＩＤ等は必要に応じて付加してもよいし、付加しなくてもよい。

【０１０８】

また、パケットのデータサイズは、固定長でもよいし、可変長でもよい。固定

長の場合、図３に示したようなダミーデータで長さを調節すればよい。

【０１０９】

上記実施形態では、本体部１のリモコン通信部１３から無線リモコン２の暗号鍵受信部への通信により、鍵情報が無線リモコン２に入力された。しかし、本発明の実施はこのような構成には限定されない。コンピュータが読み取り可能な記録媒体、例えば、フラッシュメモリカード等を介して本体部１から無線リモコン２に鍵情報を入力してもよい。

【０１１０】

その場合、本体部１に記録媒体への書き込む部（例えば、カードスロット）を設ければよい。また、無線リモコン２に、記録媒体からの読み出し部（例えば、カードスロット）を設ければよい。このような記録媒体へのアクセス装置の構成は広くしられているので、その説明は省略する。

【０１１１】

上記実施形態では、暗号鍵とセッションＩＤとにより入力情報を暗号化した。しかし、本発明の実施はこのような手順には限定されない。例えば、セッションＩＤを用いず、暗号鍵だけで入力情報を暗号化してもよい。

【０１１２】

また、例えば、家庭にある機器すべてを一つのリモコンでコントロールする場合を考える。そのようなリモコンに上記のような暗号機能付きのものを使用した場合、エアコンのオンオフやテレビのチャンネルもパソコンの操作もすべて暗号化される。

【０１１３】

このうちエアコンのオンオフなどの信号については暗号化は必要ではなく、またエアコン側に暗号化・復号化機能を設けるのは難しい場合もある。このようなときリモコンは必要に応じて暗号化する・しないを選択し、交信を行えばよい。その場合、図２に示した暗号化オン／オフスイッチ２７をオフに設定すればよい。

【０１１４】

あるいはすべてのリモコン通信はパソコンに任せて、すべて暗号化通信を使い

、パソコンに復号をさせてものよい。その場合、パソコンがエアコンなどの機器を制御することになる。この場合はパソコンがないと、機器が制御できず、リモコンが使えない。したがって、このようなシステムの利用範囲は制限されることになる。

【０１１５】

《第２実施形態》

以下、本発明の第２実施形態を図９の図面に基いて説明する。図９は第２実施におけるホームバンキングを実行する情報システムのシステム構成図である。

【０１１６】

上記第１実施形態では、暗号機能付きの無線リモコン２と、この無線リモコン２によって操作される本体部１とからなる情報システムの構成および作用について説明した。本実施形態では、そのような情報システムをホームバンキングに適用する例を説明する。本実施形態の他の構成および作用は第１実施形態のものと同様である。そこで、同一の構成については同一の符号を付してその説明を省略する。また、必要に応じて図１から図８の図面を参照する。

【０１１７】

この情報システムは、リモコン機能付きパソコン１Ａ、そのパソコンを操作するキーボード付きリモコン２Ａ、およびＬＡＮ（Local Area Network）／ＷＡＮ（Wide Area Network）を介して接続される銀行のホストコンピュータから構成される。

【０１１８】

リモコン機能付きパソコン１Ａの構成および作用は、第１実施形態における本体部１と同様である。また、キーボード付きリモコン２Ａの構成および作用は、第１実施形態の場合の無線リモコン２と同様である。

【０１１９】

ユーザは、ホームバンキングにおいて、キーボード付きリモコン２Ａを介して暗唱番号等をリモコン機能付きパソコン１Ａに入力する。このキーボード付きリモコン２Ａからリモコン機能付きパソコン１Ａへの通信は、第１実施形態の情報システムと同様暗号化されている。このような構成により、ホームバンキング利

用時の暗唱番号等が第三者に傍受される可能性を低減することができる。

【０１２０】

なお、リモコン機能付きパソコン１Ａから銀行のホストコンピュータまでのＬＡＮ／ＷＡＮによる通信では、従来から各種方法により、セキュリティが確保されている。

【０１２１】

したがって、本実施形態のリモコン機能付きパソコン１Ａと、キーボード付きリモコン２Ａとは、従来、ホームバンキングにおいて、最もセキュリティが低かった部分をカバーする。

【０１２２】

＜変形例＞

上記第２実施形態では、暗号機能を有するキーボード付きリモコン２Ａをホームバンキングに適用する例を示した。しかし、本発明の実施は、このような適用例には限定されない。すなわち、上記のキーボード付きリモコン２Ａや第１実施形態に示した暗号機能付きの無線リモコン２は、様々な情報システムに適用できる。

【０１２３】

例えば、インターネットプロバイダに接続するときにも上記システムは適用できる。インターネットプロバイダ接続時のパスワードもクレジットカードと同様の使い方ができるからである。ネットワーク上や電話線上の暗号化については整備が進んでいるため、システム全体としてみるとリモコンの部分が最も機密の弱い部分であり、上記無線リモコン２は、このような部分のセキュリティ、すなわち、システム全体のセキュリティを向上させる。

【０１２４】

《第３実施形態》

以下、本発明の実施の形態を図１０の図面に基いて説明する。図１０は第３実施におけるオフィスのセキュリティ管理を実行する情報システムのシステム構成図である。

【０１２５】

このシステムは、オフィスの従業員が使用する入室用の電子キー２Ｂを発行する鍵情報管理パソコン１Ｂと、鍵情報の発行者を認証する認証情報入力装置３と、建物玄関の施錠管理装置と、オフィスの入り口の施錠管理装置と、これらの施錠管理装置と鍵情報管理パソコン１Ｂとを接続する鍵情報通信路から構成される。

【０１２６】

鍵情報管理パソコン１Ｂの構成は、第１実施形態における本体部１と同様である。本実施形態では、鍵情報管理パソコン１Ｂは、発行した鍵情報を発行先の電子キー２Ｂごとに管理する鍵情報管理テーブルを有している。この鍵情報管理テーブルは、鍵情報を発行した電子キー２ＢのＩＤと、発行した鍵情報を対にして記録する。

【０１２７】

認証情報入力装置３は、鍵情報を発行する発行者が正当な発行者か否かを認証するための入力装置である。この認証情報入力装置３は、例えば、指紋読み取り装置、声紋解析装置、暗証番号やパスワードを入力するキーボード等である。

【０１２８】

電子キー２Ｂは、鍵情報を記録するメモリを有している。電子キー２Ｂは、例えば、磁気ストライプを有するカード、ＩＣカード、または磁気やＩＣにより情報を記録したスティック等である。

この電子キー２Ｂの鍵情報が建物玄関の施錠装置またはオフィス入り口の施錠装置にされると、その電子キー２Ｂのキー ＩＤとその鍵情報とが鍵情報通信路を通じて鍵情報管理パソコン１Ｂに送信される。そして、そのキー ＩＤと鍵情報の組み合わせが鍵情報管理テーブルに記憶済みであった場合、鍵情報管理パソコン１Ｂから施錠装置に施錠の解除指令が送信され、施錠が解除される。

【０１２９】

この電子キー２Ｂは、建物玄関やオフィス入り口の施錠を解除する従業員に配布される。そして、新たに、そのような従業員が増加した場合、認証情報が登録されている発行者により、鍵情報が発行される。

【０１３０】

すなわち、発行者は、まず、認証情報入力装置３により、まず、自身を認証し、次に、鍵情報管理パソコン１Ｂに鍵情報の発行を指令する。これにより、鍵情報が新たな電子キー２Ｂに書き込まれる。このとき、その電子キー２ＢのＩＤと発行された鍵情報が鍵情報管理テーブルに書き込まれる。

【０１３１】

なお、電子キー２Ｂを紛失した場合には、その従業員は紛失した旨を発行者に届け出る。発行者は、その従業員に配布した電子キー２Ｂの鍵情報を鍵情報管理テーブルから抹消する。さらに、発行者は、上記と同様の手順で新たな電子キー２Ｂに鍵情報を入力し、その従業員に引き渡す。

【０１３２】

このように、本実施形態のシステムによれば、認証された発行者により簡易に電子キー２Ｂを発行することができる。また、電子キー２Ｂを紛失したような場合も、他の従業員に影響を与えることなく、紛失した電子キー２Ｂを無効にすることができる。

【０１３３】

《コンピュータ読み取り可能な記録媒体》

上記実施の形態におけるいずれかの処理をコンピュータに実行させるプログラムをコンピュータ読み取り可能な記録媒体に記録することができる。そして、コンピュータに、この記録媒体のプログラムを読み込ませて実行させることにより、上記実施の形態に示した本体部１、リモコン機能付きパソコン１Ａ、暗号鍵発行装置１Ｂ、無線リモコン２、または、キーボード付きリモコン２Ａの機能を提供させることができる。

【０１３４】

ここで、コンピュータ読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的、または化学的作用によって蓄積し、コンピュータから読み取ることができる記録媒体をいう。このような記録媒体のうちコンピュータから取り外し可能なものとしては、例えばフロッピーディスク、光磁気ディスク、CD-ROM、CD-R/W、DVD、DAT、８mmテープ、メモリカード等がある。

【０１３５】

また、コンピュータに固定された記録媒体としてハードディスクやＲＯＭ（リードオンリーメモリ）等がある。

【０１３６】

《搬送波に具現化されたデータ通信信号》

また、上記プログラムをコンピュータのハードディスクやメモリに格納し、通信媒体を通じて他のコンピュータに配布することができる。この場合、プログラムは、搬送波によって具現化されたデータ通信信号として、通信媒体を伝送される。そして、その配布を受けたコンピュータに上記本体部１、リモコン機能付きパソコン１Ａ、暗号鍵発行装置１Ｂ、無線リモコン２、または、キーボード付きリモコン２Ａの機能を提供させることができる。

【０１３７】

ここで通信媒体としては、有線通信媒体、例えば、同軸ケーブルおよびツイストペアケーブルを含む金属ケーブル類、光通信ケーブル等、または、無線通信媒体例えば、衛星通信、地上波無線通信等のいずれでもよい。

【０１３８】

また、搬送波は、データ通信信号を変調するための電磁波または光である。ただし、搬送波は、直流信号でもよい。この場合、データ通信信号は、搬送波がないベースバンド波形になる。したがって、搬送波に具現化されたデータ通信信号は、変調されたブロードバンド信号と変調されていないベースバンド信号（電圧０の直流信号を搬送波とした場合に相当）のいずれでもよい。

【０１３９】

《その他》

さらに、本実施の形態は以下の発明を開示する。

【０１４０】

（付記１）　鍵情報保持装置に鍵情報を発行する鍵情報発行装置であり、

前記鍵情報の発行者を認証する認証部と、

前記鍵情報保持装置に鍵情報を出力する出力部と、

発行された鍵情報を前記鍵情報保持装置に対応付けて記録する記録部とを備え

、認証された発行者の指示により鍵情報を発行する鍵情報発行装置。（１）

【０１４１】

（付記２）　前記鍵情報保持装置は、情報機器に無線で接続される無線操作装置であり、前鍵情報発行装置に接触して鍵情報を入力する鍵情報入力部を有しており、

前記出力部は、前記鍵情報入力部と接触して鍵情報を出力する接触部を有し、その接触部を介して鍵情報を発行する付記１記載の鍵情報発行装置。（２）

【０１４２】

（付記３）　前記鍵情報保持装置は、情報機器に無線で接続される無線操作装置であり、記録媒体から情報を入力する媒体入力部を有しており、

前記出力部は、前記記録媒体に情報書き込む記録媒体書き込み部を有し、その記録媒体を介して鍵情報を発行する付記１記載の鍵情報発行装置。

【０１４３】

（付記４）　前記鍵情報保持装置は、情報機器に無線で接続される無線操作装置であり、所定距離外では通信できない近接通信部を有しており、

前記出力部は、前記鍵情報保持装置と所定距離外では通信できない近接通信部を有し、その近接通信部を介して鍵情報を発行する付記１記載の鍵情報発行装置。

【０１４４】

（付記５）　前記鍵情報保持装置からの無線信号を受信する受信部と、

前記無線信号に含まれる、前記暗号鍵情報により暗号化された情報を復号する復号部とをさらに備える付記１記載の鍵情報発行装置。

【０１４５】

（付記６）　情報機器に無線で接続される無線操作装置であり、

情報を暗号化するための鍵情報を入力する鍵情報入力部と、

前記鍵情報を記録する記録部と、

利用者の操作を検出する操作部と、

前記操作による入力情報を前記鍵情報により暗号化する暗号化部と、

暗号化された入力情報を情報機器に送信する送信部とを備える無線操作装置。

（３）

【０１４６】

（付記７）　前記鍵情報入力部は、前記鍵情報を接触して入力する接触部を有する付記６記載の無線操作装置。

【０１４７】

（付記８）　前記鍵情報入力部は、記録媒体から情報を入力する媒体入力部を有する付記６記載の無線操作装置。

【０１４８】

（付記９）　前記鍵情報入力部は、所定距離外では通信できない近接通信部を有する付記６記載の無線操作装置。

【０１４９】

（付記１０）　暗号化の有無を設定する設定部をさらに備え、

前記暗号化部は、暗号化が指示されているときに入力情報を暗号化する付記６記載の無線操作装置。

【０１５０】

（付記１１）　情報機器に無線で接続される無線操作装置であり、

利用者の操作を検出する操作部と、

前記操作による入力情報を送信する送信部と、

送信した入力情報に対する前記情報機器からの応答信号の有無を確認する確認部とを備え、前記応答信号が得られない場合に、入力情報の送信を停止する無線操作装置。

【０１５１】

（付記１２）　情報機器に無線で接続される無線操作装置であり、

利用者の操作を検出し、入力情報を生成する操作部と、

前記入力情報を模擬した模擬情報を発生する模擬情報発生部と、

前記入力情報または模擬情報を送信する送信部とを備える無線操作装置。

【０１５２】

（付記１３）　前記模擬情報は、利用者による操作の有無に拘わらず送信される付記１２記載の無線操作装置。

【０１５３】

（付記１４）　前記鍵情報保持装置は、所定領域の施錠を開放する電子鍵である付記１記載の鍵情報発行装置。（４）

【０１５４】

（付記１５）　鍵情報保持装置に発行される鍵情報を管理する方法であり、

前記鍵情報の発行者を認証するステップと、

鍵情報を生成するステップと、

前記鍵情報保持装置に鍵情報を出力するステップと、

発行された鍵情報を前記鍵情報保持装置に対応付けて記録するステップとを有する鍵情報を管理する方法。

【０１５５】

（付記１６）　前記鍵情報保持装置は、情報機器に無線で接続される無線入力装置であり、接触して情報を入力する入力部を有しており、

前記出力するステップは、その入力部を介して鍵情報を発行する付記１５記載の鍵情報を管理する方法。

【０１５６】

（付記１７）　前記鍵情報保持装置は、情報機器に無線で接続される無線入力装置であり、記録媒体から情報を入力する媒体入力部を有しており、

前記出力するステップは、前記記録媒体に情報を書き込むステップを有し、その記録媒体を介して鍵情報を発行する付記１５記載の鍵情報を管理する方法。

【０１５７】

（付記１８）　前記鍵情報保持装置は、情報機器に無線で接続される無線入力装置であり、所定距離外では通信できない近接通信部を有しており、

前記出力するステップは、その近接通信部を介して鍵情報を発行する付記１５記載の鍵情報を管理する方法。

【０１５８】

（付記１９）　前記鍵情報保持装置からの無線信号を受信するステップと、

前記無線信号に含まれる、前記暗号鍵情報により暗号化された情報を復号するステップとをさらに有する付記１５記載の鍵情報を管理する方法。

【０１５９】

（付記２０）　無線信号による機器制御方法であり、

情報を暗号化するための鍵情報を入力するステップと、

前記暗号化のための鍵情報を記録するステップと、

利用者の操作を検出するステップと、

前記操作による入力情報を前記鍵情報により暗号化するステップと、

暗号化された入力情報を無線信号で送信するステップとを有する機器制御方法。

【０１６０】

（付記２１）　前記鍵情報を入力するステップは、前記無線信号とは異なる接触信号により前記鍵情報を入力する付記２０記載の機器制御方法。

【０１６１】

（付記２２）　前記鍵情報を入力するステップは、記録媒体から鍵情報を入力する付記２０記載の機器制御方法。

【０１６２】

（付記２３）　前記鍵情報を入力するステップは、所定距離外では通信できない近接通信により鍵情報を入力する付記２０記載の機器制御方法。

【０１６３】

（付記２４）　暗号化の有無を設定するステップをさらに備え、

前記暗号化するステップは、暗号化が指示されているときに前記入力情報を暗号化する付記２０記載の機器制御方法。

【０１６４】

（付記２５）　無線信号による機器制御方法であり、

利用者の操作を検出するステップと、

前記操作による入力情報を送信するステップと、

送信した入力情報に対する応答信号の有無を確認するステップと、

前記応答信号が得られない場合に、入力情報の送信を停止するステップとを有する機器制御方法。

【０１６５】

（付記２６）　無線信号による機器制御方法であり、

利用者の操作を検出し、入力情報を生成するステップと、

前記入力情報を模擬した模擬情報を発生するステップと、

前記入力情報を送信するステップと、

前記模擬情報を送信するステップとを有する機器制御方法。

【０１６６】

（付記２７）　前記模擬情報は、利用者による操作の有無に拘わらず送信される付記２６記載の機器制御方法。

【０１６７】

（付記２８）　前記鍵情報保持装置は、所定領域の施錠を開放する電子鍵である付記１５記載の鍵情報を管理する方法。

【０１６８】

（付記２９）　コンピュータに、鍵情報保持装置に発行される鍵情報を管理させるプログラムであり、

前記鍵情報の発行者を認証するステップと、

鍵情報を生成するステップと、

前記鍵情報保持装置に鍵情報を出力するステップと、

発行された鍵情報を前記鍵情報保持装置に対応付けて記録するステップとを有するプログラム。（５）

【０１６９】

（付記３０）　前記鍵情報保持装置は、情報機器に無線で接続される無線入力装置であり、接触して情報を入力する入力部を有しており、

前記出力するステップは、その入力部を介して鍵情報を発行させる付記２９記載のプログラム。

【０１７０】

（付記３１）　前記鍵情報保持装置は、情報機器に無線で接続される無線入力装置であり、記録媒体から情報を入力する媒体入力部を有しており、

前記出力するステップは、前記記録媒体に情報を書き込むステップを有し、その記録媒体を介して鍵情報を発行させる付記２９記載のプログラム。

【０１７１】

（付記３２）　前記鍵情報保持装置は、情報機器に無線で接続される無線入力装置であり、所定距離外では通信できない近接通信部を有しており、

前記出力するステップは、その近接通信部を介して鍵情報を発行させる付記２９記載のプログラム。

【０１７２】

（付記３３）　前記鍵情報保持装置からの無線信号を受信するステップと、

前記無線信号に含まれる、前記暗号鍵情報により暗号化された情報を復号するステップとをさらに有する付記２９記載のプログラム。

【０１７３】

（付記３４）　コンピュータに、無線信号による機器制御を実行させるプログラムであり、

情報を暗号化するための鍵情報を入力するステップと、

前記暗号化のための鍵情報を記録するステップと、

利用者の操作を検出するステップと、

前記操作による入力情報を前記鍵情報により暗号化するステップと、

暗号化された入力情報を無線信号で送信するステップとを有するプログラム。

【０１７４】

（付記３５）　前記鍵情報を入力するステップは、前記無線信号とは異なる接触信号により前記鍵情報を入力させる付記３４記載のプログラム。

【０１７５】

（付記３６）　前記鍵情報を入力するステップは、記録媒体から鍵情報を入力させる付記３４記載のプログラム。

【０１７６】

（付記３７）　前記鍵情報を入力するステップは、所定距離外では通信できない近接通信により鍵情報を入力させる付記３４記載のプログラム。

【０１７７】

（付記３８）　暗号化の有無を設定するステップをさらに備え、

前記暗号化するステップは、暗号化が指示されているときに前記入力情報を暗

号化させる付記３４記載のプログラム。

【０１７８】

（付記３９）　コンピュータに、無線信号による機器制御を実行させるプログラムであり、

利用者の操作を検出するステップと、

前記操作による入力情報を送信するステップと、

送信した入力情報に対する応答信号の有無を確認するステップと、

前記応答信号が得られない場合に、入力情報の送信を停止するステップとを有するプログラム。

【０１７９】

（付記４０）　コンピュータに、無線信号による機器制御を実行させるプログラムであり、

利用者の操作を検出し、入力情報を生成するステップと、

前記入力情報を模擬した模擬情報を発生するステップと、

前記入力情報を送信するステップと、

前記模擬情報を送信するステップとを有するプログラム。

【０１８０】

（付記４１）　前記模擬情報は、利用者による操作の有無に拘わらず送信される付記４０記載のプログラム。

【０１８１】

（付記４２）　前記鍵情報保持装置は、所定領域の施錠を開放する電子鍵である付記２９記載の鍵情報を管理するプログラム。

【０１８２】

（付記４３）　コンピュータに、鍵情報保持装置に発行される鍵情報を管理させるプログラムであり、

前記鍵情報の発行者を認証するステップと、

鍵情報を生成するステップと、

前記鍵情報保持装置に鍵情報を出力するステップと、

発行された鍵情報を前記鍵情報保持装置に対応付けて記録するステップとを有

するプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０１８３】

【発明の効果】

以上説明したように、本発明によれば、情報機器と無線リモコンとの間の通信で傍受からの十分な安全性を確保することができる。本発明によれば、鍵情報を保持する鍵情報保持装置に対して簡易に鍵情報を発行することができる。また、本発明によれば、そのような鍵情報の発行において、傍受からの十分な安全性を確保することができる。

【図面の簡単な説明】

【図１】　本発明の第１実施形態に係る情報システムの全体図

【図２】　リモコン２のブロック図

【図３】　パケットのデータ構造図

【図４】　本体部１からリモコン２へ暗号鍵を配布する手順を示すフローチャート

【図５】　リモコン動作時の処理を示すフローチャート

【図６】　ボタン情報暗号化の処理の詳細を示すフローチャート

【図７】　ボタン情報パケット、ダミーパケット送出処理の詳細を示すフローチャート

【図８】　本体部１の受信動作時の処理を示すフローチャート

【図９】　本発明の第２実施におけるホームバンキングを実行する情報システムのシステム構成図

【図１０】本発明の第３実施におけるオフィスのセキュリティ管理を実行する情報システムのシステム構成図

【符号の説明】

１　　本体部

１Ａ　リモコン機能付きパソコン

１Ｂ　鍵情報管理パソコン

２　　無線リモコン

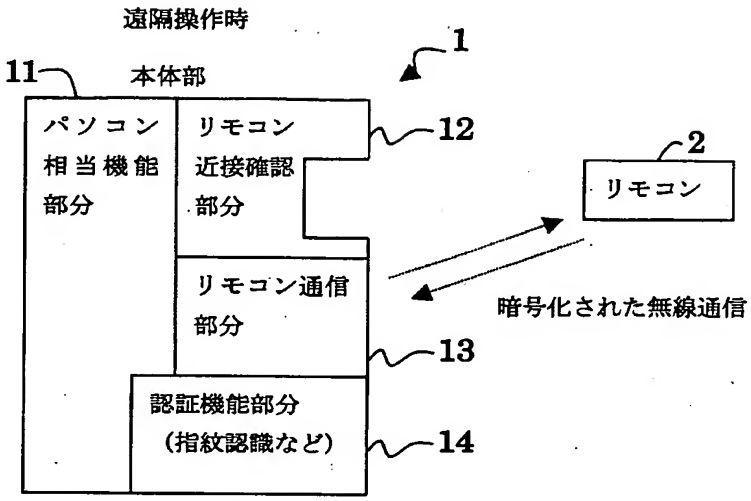
２Ａ　キーボード付きリモコン

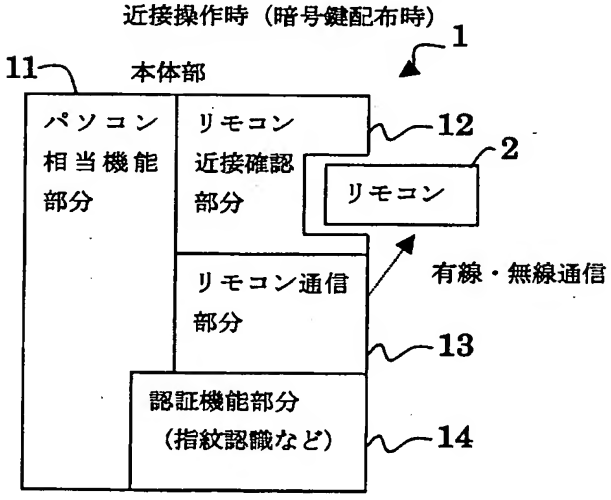
２Ｂ　電子キー
３　認証情報入力装置
１１　パソコン相当機能部分
１２　リモコン近接確認部分
１３　リモコン通信部分
１４　認証機能部分
２１　処理装置
２２　キーボード
２３　暗号鍵受信部
２４　メモリ
２５　送受信装置
２７　暗号化オン／オフスイッチ

【書類名】　　図面

【図１】

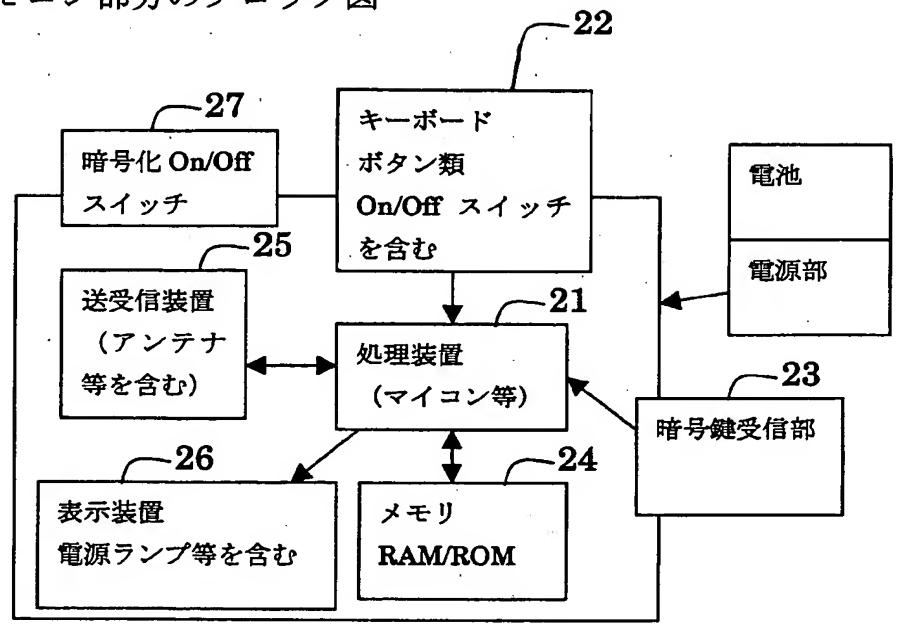
全体図


遠隔操作時
1
11
本体部
パソコン相当機能部分
リモコン近接確認部分
12
2
リモコン
リモコン通信部分
暗号化された無線通信
13
認証機能部分（指紋認識など）
14


近接操作時（暗号鍵配布時）
1
11
本体部
パソコン相当機能部分
リモコン近接確認部分
12
2
リモコン
リモコン通信部分
有線・無線通信
13
認証機能部分（指紋認識など）
14

【図２】

リモコン部分のブロック図



【図３】

パケットのデータ構造例

交信開始パケットの例

	ヘッダ	パケットID	リモコンID	ダミーデータ	チェックサム	
	55AA	0000	12345678	0000000000...	3F	

交信許可パケットの例

	ヘッダ	パケットID	リモコンID	セッションID	ダミーデータ	チェックサム	
	55AA	0001	12345678	41943786	00...	61	

ボタン情報・ダミーパケットの例

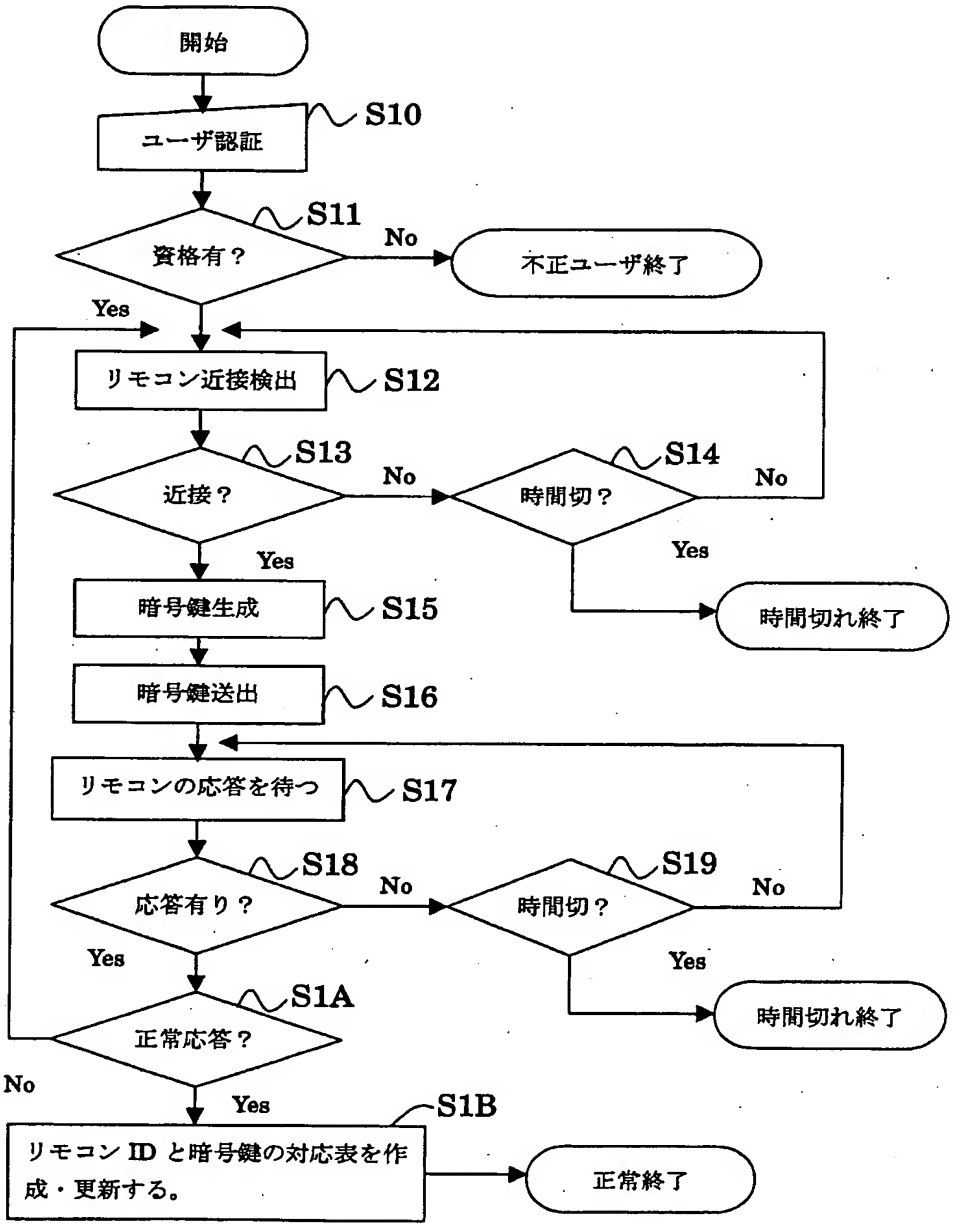
	ヘッダ	パケットID	リモコンID	暗号化されたボタン情報またはダミー	チェックサム	
	55AA	0002	12345678	01987d4fa34f45a09185b197	8b	

受信確認パケットの例

	ヘッダ	パケットID	リモコンID	受信パケットのチェックサム	次セッションID	チェックサム	
	55AA	0003	12345678	8b	9858950	C4	

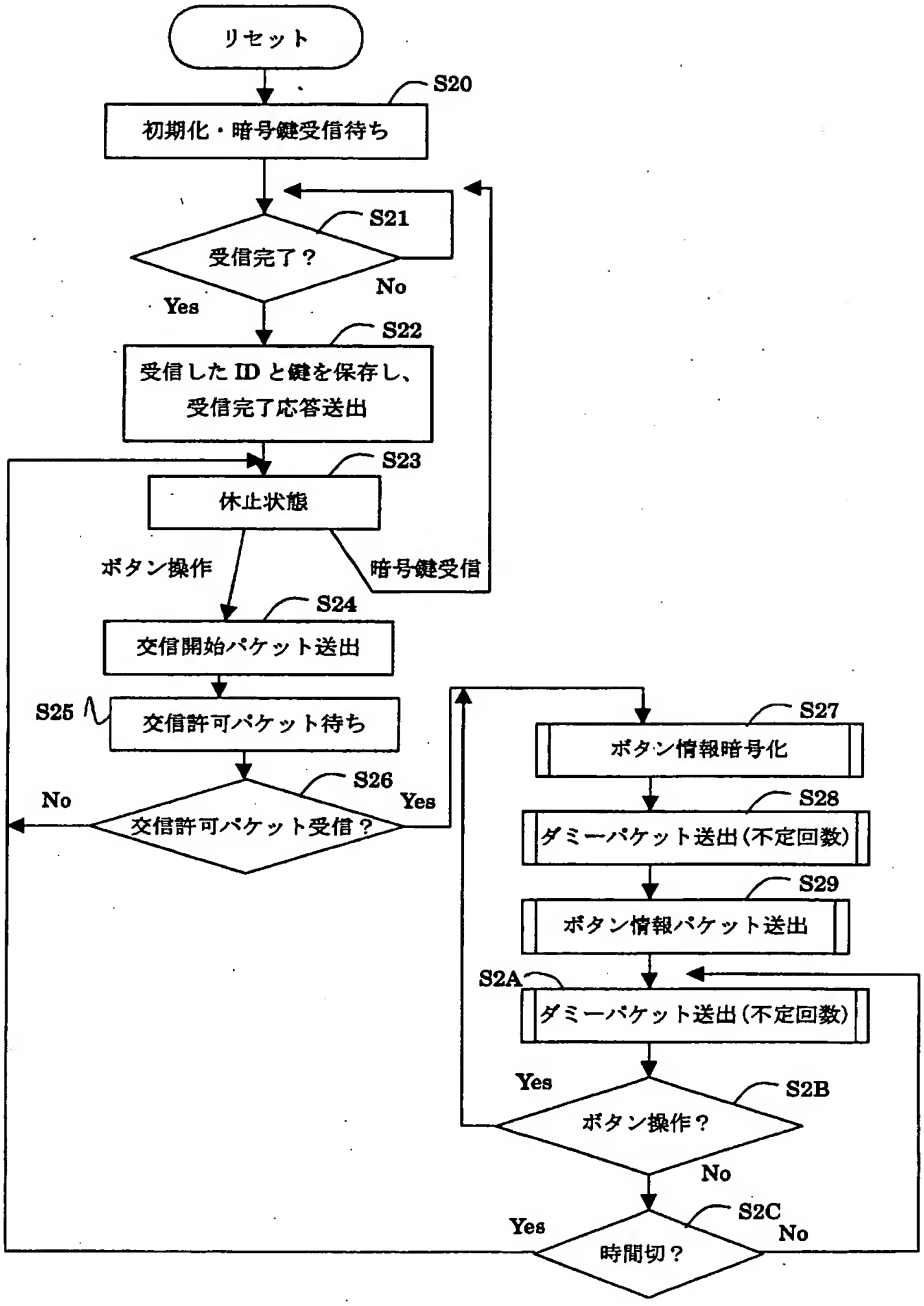
【図４】

暗号鍵配布手順フローチャート（例）



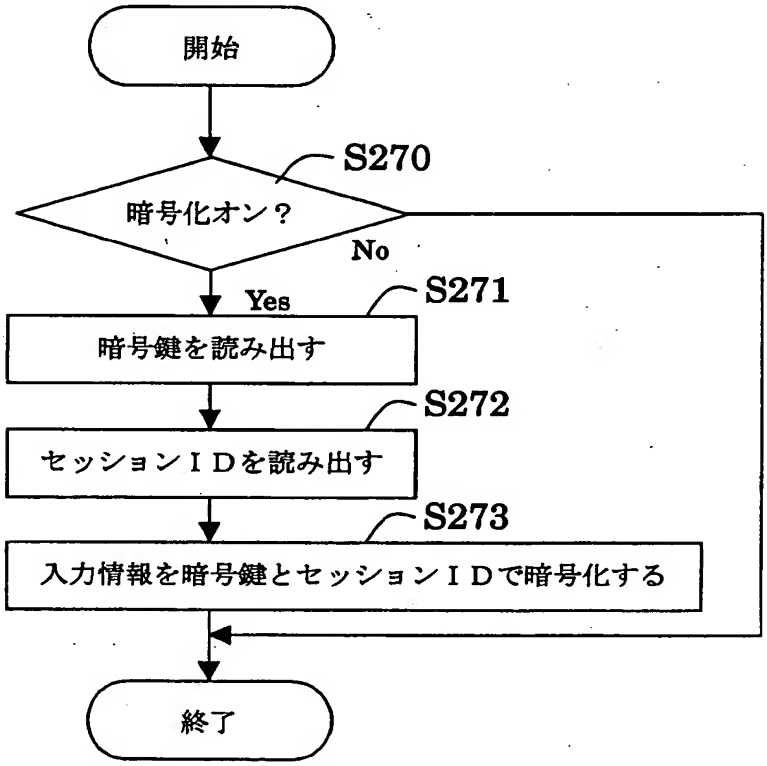
【図５】

リモコン動作フローチャート（例）



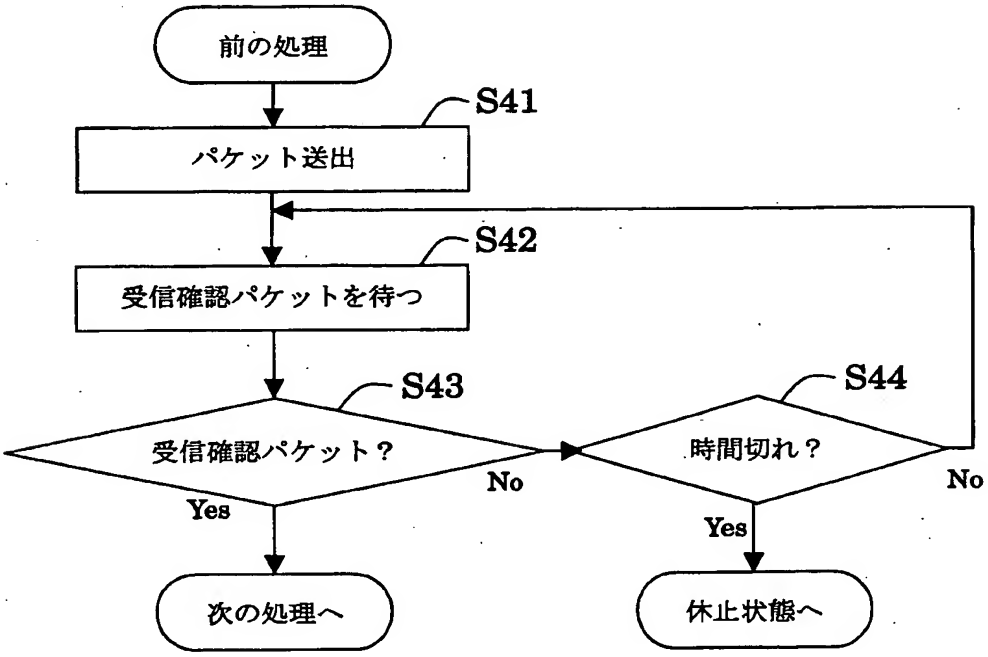
【図６】

ボタン情報暗号化処理フローチャート



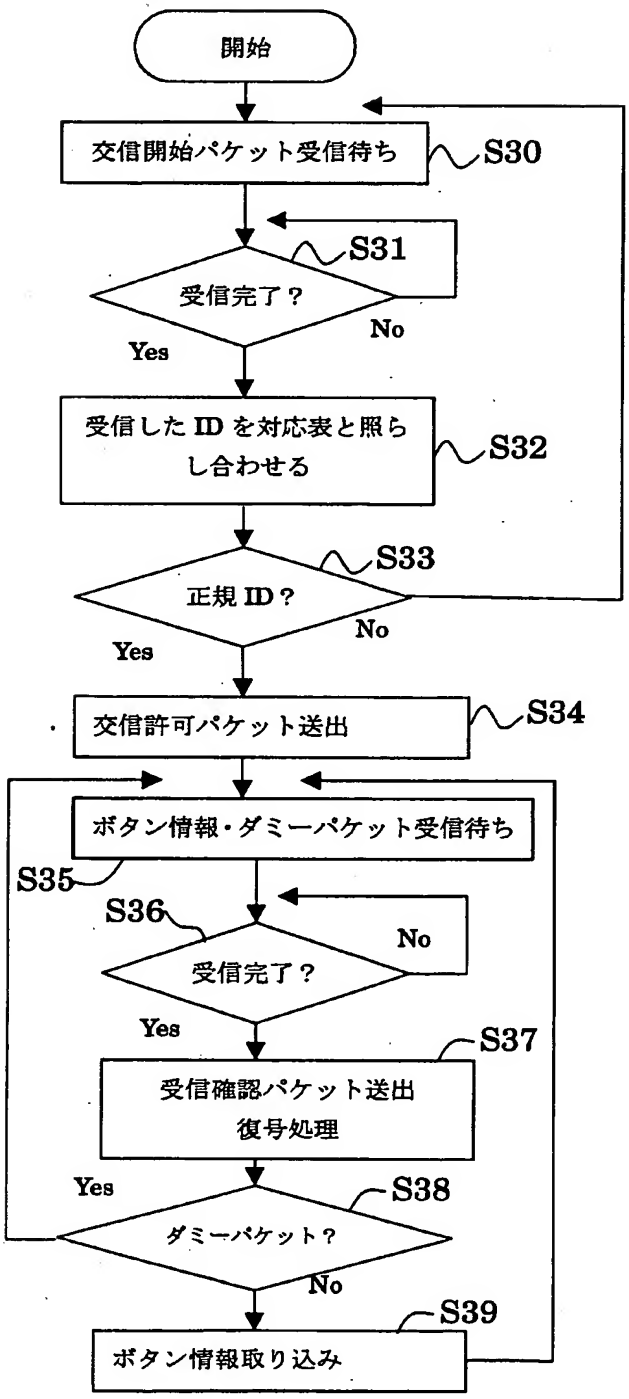
【図７】

ボタン情報パケット、ダミーパケット送出フローチャート

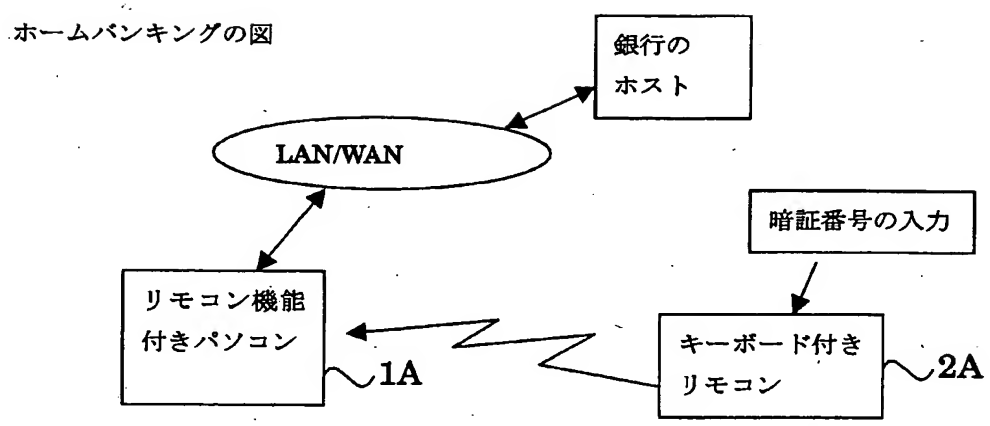


【図８】

本体部１の受信動作フローチャート

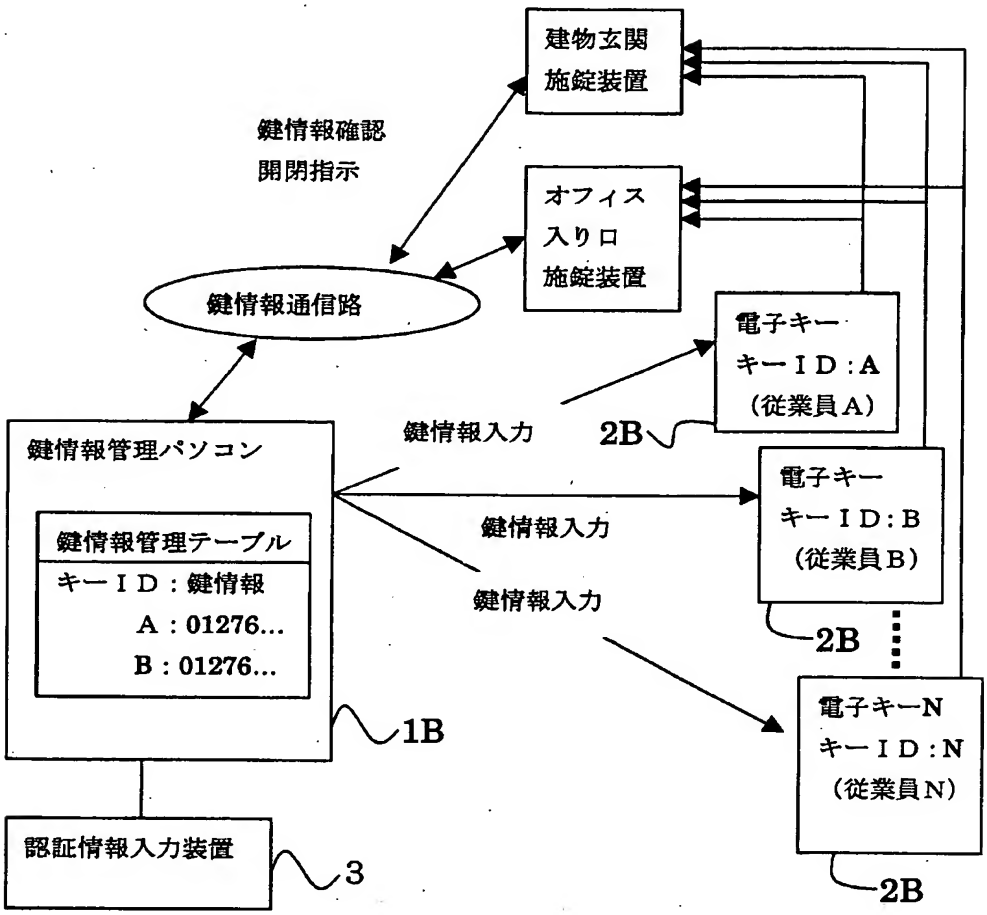


【図９】


ホームバンキングの図
銀行の
ホスト
LAN/WAN
暗証番号の入力
リモコン機能
付きパソコン
1A
キーボード付き
リモコン
2A

【図１０】

オフィスの施錠管理のシステム構成図



【書類名】　　要約書

【要約】

【課題】

情報機器と無線操作装置との間の通信において傍受からの十分な安全性を確保する。

【解決手段】

鍵情報保持装置（２、２Ａ、２Ｂ）に鍵情報を発行する鍵情報発行装置（１、１Ａ、１Ｂ）であり、

鍵情報の発行者を認証する認証部（１４、３）と、

上記鍵情報保持装置に鍵情報を出力する出力部（１３）と、

発行された鍵情報を上記鍵情報保持装置に対応付けて記録する記録部（１１）とを備え、認証された発行者の指示により鍵情報を発行する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社